REMARKS

This application has been carefully reviewed in light of the Office Action dated November 26, 2003 (Paper No. 6) and the Advisory Action dated March 18, 2004 (Paper No. 8). Claims 1 to 51 are pending in the application. Claims 1, 10, 18, 27, 35 and 44, the independent claims, have been amended. Reconsideration and further examination are respectfully requested.

A first Amendment After Final Rejection, dated February 26, 2004, was denied entry in the Advisory Action. In a follow-up telephone interview concerning the Advisory Action, the Examiner explained that entry had been denied because deletion of the word "automatically" broadened the claims, which was not permissible after a final rejection. Based on the interview, the word "automatically" is retained in the Second Amendment After Final Rejection, although other changes have been made.

Further in this regard, since the first Amendment was denied entry, the changes in this second Amendment are made relative to the claim wording in the Amendment dated October 30, 2003.

Claims 1 to 51 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 6,181,440 (Masuda) in view of U.S. Patent No. 4,992,783 (Zdunek); and Claims 35 to 51 were rejected under 35 U.S.C. § 103(a) over Masuda in view of Zdunek and further in view of U.S. Patent No. 5,764,807 (Pearlman). Reconsideration and withdrawal of the rejections are respectfully requested.

The present invention generally concerns the retrieval of document data, in which a request for retrieval of document data is received from a user, with the request including a password. The stored document data is retrieved and the document data is

output. According to one feature of the invention, a new password is automatically issued in response to receiving from the user the request for retrieval of the document data, and the user is notified of the new password if the user is authorized.

By virtue of the foregoing, in which a new password is automatically issued in response to receiving from the user the request for retrieval of the document data, and the user is notified of the new password if the user is authorized, an authorized user retains his ability to access document data, even though the password has been changed, since he is notified of the new password.

Referring specifically to the claims, independent Claim 1 as amended is directed to an apparatus for conducting a retrieval of document data including storing means for storing the document data, a receiver, for receiving from a user a request for retrieval of the document data, with the request including a password, and a transmitter, for transmitting the password, received by the receiver, to a managing unit on a network. The apparatus also includes deciding means for, when the managing unit confirms the password transmitted by the transmitter, receiving a confirmation result from the managing unit to decide, on the basis of the confirmation result, whether or not the user is an authorized user. In addition, the apparatus includes retrieving means for retrieving the document data stored in the storing means according to a decision result obtained by the deciding means, and outputting means for outputting document data retrieved by the retrieving means. The apparatus also includes issuing means for issuing a new password automatically in response to receiving from the user the request for retrieval of the document data by the receiver, wherein the user is notified of the new password if the user is authorized. In addition, the apparatus includes registering means for transmitting the new password,

issued by the issuing means, to the managing unit to register the new password as a valid password.

In a similar manner, independent Claims 18 and 35 as amended respectively define the invention in terms of a method and a record medium storing a computer program.

Independent Claim 10 as amended is directed to an apparatus for conducting a retrieval of document data. The apparatus includes storing means for storing the document data, a receiver, for receiving a request for a retrieval of the document data, including a password, from a user, and confirming means for confirming authorization of the user through the use of the password which the receiver receives. The apparatus also includes retrieving means for retrieving the document data stored in the storing means on the basis of a confirmation result by the confirming means, and outputting means for outputting document data retrieved by the retrieving means. In addition, the apparatus includes issuing means for issuing a new password automatically in response to a receiving operation of the receiving means, wherein the user is notified of the new password if the user is authorized. The apparatus also includes notifying means for notifying the user of the new password issued by the issuing means in a mode corresponding to a mode taken for when the receiver receives the retrieval request.

In a similar manner, independent Claims 27 and 44 as amended respectively define the invention in terms of a method and a record medium storing a computer program.

The applied art is not seen to disclose or suggest the features of the present invention. In particular, the applied art is not seen to provide for issuing a new password

automatically in response to receiving from the user the request for retrieval of the document data, wherein the user is notified of the new password if the user is authorized.

Masuda discloses a facsimile apparatus, which includes a printer, a memory, a reception unit, and a setting unit. See Masuda, Abstract; column 2, line 63 to column 3, line 4; and Figure 1. As acknowledged in the Office Action, however, Masuda does not disclose issuing a new password in response to receiving from the user the request for retrieval of the document data.

Zdunek was cited for its alleged disclosure of issuing a new password in response to receiving a document retrieval request from a user. As understood by Applicant, Zdunek discloses a communication system in which subscribers use a password for access to communication resources. Subscribers are required to modify their password either periodically or upon requesting access to the communication system, or can opt to have the new password automatically generated after the expiration of a timer or the occurrence of some event. The modified password is retained as the current password by both the subscriber and the communication system. See Abstract; column 8, line 63 to column 9, line 12; and Fig. 4.

However, Zdunek does not teach issuing a new password automatically in response to receiving from the user the request for retrieval of the document data, wherein the user is notified of the new password if the user is authorized.

First, Zdunek is silent as to whether authorized users are notified of new passwords that are automatically generated. In Zdunek, authorized users who choose to manually modify their password are commanded to do so either periodically or upon requesting access to the system. In this manner, the authorized users of Zdunek are able to

maintain the current password, and unauthorized users eventually become out-of-sync with the system. However, Zdunek is silent as to how passwords are maintained when a user opts to have new passwords automatically generated. Zdunek does not describe the notification of the new password, and therefore could not possibly describe that the user is notified of the new password if the user is authorized.

In addition, Zdunek automatically generates a new password at the expiration of a timer or occurrence of some unarticulated event, and not in response to receiving from the user the request for retrieval of the document data.

As such, even if Masuda and Zdunek are combined in the manner proposed in the Office Action (assuming for argument's sake that such combination would be permissible), the result would not teach at least the feature of issuing a new password automatically in response to receiving from the user the request for retrieval of the document data, wherein the user is notified of the new password if the user is authorized, nor would it suggest the attendant benefits provided by issuing a new password in this manner.

In addition, Pearlman has been reviewed and is not seen to compensate for the deficiencies of Masuda and Zdunek.

Accordingly, based on the foregoing remarks, independent Claims 1, 10, 18, 27, 35 and 44 are believed to be allowable over the applied references. Reconsideration and withdrawal of the § 103(a) rejections are respectfully requested.

The other claims in the application are each dependent from the independent claims and are believed to be allowable over the applied references for at least the same reasons. Because each dependent claim is deemed to define an additional aspect of the

invention, however, the individual consideration of each on its own merits is respectfully requested.

No other matters being raised, it is believed that the entire application is fully in condition for allowance, and such action is courteously solicited.

Applicant's undersigned attorney may be reached in our Costa Mesa, California office at (714) 540-8700. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant

Registration No. 32,622

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-2200
Facsimile: (212) 218-2200

CA_MAIN 79553v1